REMARKS

Applicants appreciate the thorough examination of the present application as evidenced by the final Office Action mailed October 10, 2008 (hereinafter "Office Action"). In response, Applicants have amended independent Claims 46, 59 and 69. Applicants respectfully submit that no new matter is added and support for this amendment may be found in the Specification at page 3, lines 22-25, among others. Applicants respectfully submit that currently pending Claims 46-75 are allowable over the cited references for at least the reasons provided below. Accordingly, Applicants respectfully request a Notice of Allowance in due course.

Claims 46, 59 and 69 are Patentable Over SyncML

The Office Action rejects Claims 46-49, 54-56, 59-62 and 67-71 under 35 U.S.C. §102(b) as being anticipated by SyncML Sync Protocol, version 1.0, SYNCML CONSORTIUM, published December 7, 2000 (hereinafter "SyncML"). (Office Action, page 3.) Applicants respectfully submit that independent Claims 46, 59 and 69, as amended, are patentable over SyncML for at least the reasons that SyncML does not disclose or suggest the recitations therein. For example, independent Claim 46, as amended, recites:

> A method for providing authentication when messages are sent between an electronic communication apparatus and a server according to a synchronization protocol in which a plurality of different authentication methods, among which **a subset comprises addition authentication methods**, comprising:
> providing an authentication method indicator that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed;
> **incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods**; and
> transmitting said message to said server according to an authentication protocol of the synchronization protocol. (*Emphasis added.*)

In rejecting Claim 46, the Office Action states that SyncML discloses:

> incorporating into a message the authentication method indicator

> *(pages 21-24, section 3.5.1; XML Tag 'type'; page 23; XML Tag 'type' <auth-md5>; page 13, section 2.5; both the sync client and server can challenge for the authentication and the device receiving the authentication challenge must be able to send the authentication credentials back; see also pages 26-30 and 34-40)* comprising a plurality of authentication capabilities of the communication apparatus *(page 13, section 2.5; the protocol requires the support for the basic authentication and the MD5 digest access authentication; pages 21-24, section 3.5.1; xml Tag 'type' ,auth-basic>; XML Tag 'type' <auth-md5>; see also pages 26-30 and 34-40).*

(Office Action, page 4.) Applicants respectfully submit that SyncML provides that basic and MD5 digest authentication must be supported by the devices. For example, SyncML at Chapter 3 states that "[b]oth of them MUST be supported by the devices conforming to this specification." Accordingly, SyncML provides that when MD5 digest access is already determined, the server includes the MD5 type in the authentication request, which is thus obeyed by the client. In contrast with the present invention, SyncML describes authentication that may have little or no flexibility.

By way of explanation, the Basic scheme may be described as a Base64 character encoding of the concatenation of the orginator's user id, followed by a colon separator character, which may be followed by the password associated with the specified user id. This authentication scheme may be simple to implement, but may be susceptible to network eavesdropping.

The MD5 digest form of concatenation may be described as an authentication identifier such as the originator's user id, followed by the colon separator character, which may be followed by some secret known by the originator and the recipient such as the originator's password for the corresponding user id, which may further be followed by a recipient specified nonce string. The maximum duration that the nonce string may be used may be the current SyncML session. More frequent changes to the nonce string may be specified with the NextNonce element type within the Meta element type of the Chal element type. The MD5 credential, a 128-bit binary digest value, may require BASE64 character encoding when transferred as clear-text XML. Applicants note that both the Basic and MD5 digest authentication schemes are mandatory authentication methods supported in SyncML.

In contrast, Applicants respectfully submit that SyncML does not disclose or suggest, for example, "incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus **among the plurality of different authentication methods**," as recited in Claim 46, as amended. Claim 46 is amended to clarify that a set of authentication methods, a subset of which are addition authentication methods, is available for use in a synchronization protocol. In this regard, SyncML does not contemplate the use of addition authentication methods, which may be optional authentication methods. Thus SyncML does not disclose or suggest "incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods," as recited in Claim 46, as amended.

Additionally, Applicants respectfully submit that the "plurality of authentication capabilities of the communication apparatus" is wholly distinct from the operations described above regarding SyncML. For example, the operations according to SyncML require two additional transmissions to establish the synchronization relative to the operations recited in Claim 46, as amended.

Further, Claim 46, as amended, recites "incorporating into **a message**" and "transmitting the message **to said server**." In this regard, the "message" is a message from the apparatus. According to the Office Action allegation, the cited portions of SyncML that are interpreted as disclosing "the authentication method indicator" are included in packages **from** the server to the apparatus and not vice versa. SyncML, sections 3.5.1 and 3.5.2. In this regard, the cited portions of SyncML are not in the message of Claim 46 that is transmitted "to said server." Thus, SyncML does not disclose or suggest "incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods," as recited in Claim 46, as amended.

Accordingly, Applicants respectfully submit that independent Claim 46, as amended, is patentable over SyncML for at least these reasons, the allowance of which is respectfully requested. Applicants further submit that independent Claims 59 and 69, as amended,

include similar recitations and are thus patentable over SyncML for at least the same reasons.

Dependent claims are patentable

Applicants respectfully submit that dependent Claims 46-58, 60-68 and 70-75 are patentable at least per the patentability of the independent claims from which they depend.

In re: Gustavsson et al.
Application No.: 10/506,943
Filed: March 7, 2005
Page 13

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.
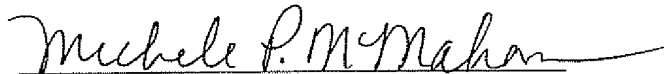
Respectfully submitted,

Timothy J. Wall
Registration No.: 50,743

USPTO Customer No. 54414
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401